REMARKS

The September 14, 2007 Office Action regarding the above-identified application has been carefully considered; and the claim amendments above together with the remarks that follow are presented in a bona fide effort to respond thereto and address all issues raised in that Action. The independent claims have been amended to address an indefiniteness rejection in the latest Office Action. It is believed that the revised claim language only provides improved clarity and as such does not narrow the scope of any amended claim. New dependent claims have been added above. Care has been taken to avoid entry of new matter. For reasons discussed below, it is believed that this case is in condition for allowance. Prompt favorable reconsideration of this amended application is requested.

The Office Action rejected claims 1, 3-8 and 10-14 as indefinite, on the ground that the previous recitations in claims 1 and 8 of "verifying the generated item of information" for each respective partial document, and "based on a result of the item verifying," determining whether each respective partial document has been deleted or modified were confusing. The last paragraph of each independent claim has been amended to clarify this point. Each independent claim 1 or 8 now recites "determining whether each respective partial document has been deleted or modified based on the verifying of the generated item of information for the respective partial document." The "result" term has been deleted, and it is believed that one of skill in the art would understand that the determination with regard to each respective partial document is responsive to or "based on" the step or function of verifying of the generated item of information for that respective partial document. Hence, the amended independent claims are reasonably clear, concise and definite; and the indefiniteness rejection should be withdrawn.

Claims 1 and 8 also were rejected under 35 U.S.C. § 101 for alleged lack of utility. Applicants respectfully traverse this rejection. Claim 1 relates to an electronic document

management system, and claim 8 relates to an electronic document management method. Document management is clearly useful. Both of the claims include recitations relating to verifying the validity of a masked electronic document. It is respectfully submitted that verifying document validity also is useful, in the context of document management; and such a result is tangible, concrete and provides utility particularly in that context. Document management and verification of validity of a managed document are not abstract concepts. Hence, it is respectfully submitted that claims 1 and 8 do in fact recite patentable subject matter under U.S.C. § 101 that provides clear utility. Hence, the rejection under this section of the statute is improper and should be withdrawn.

Claims 1, 4-8 and 11-14 stand rejected under 35 U.S.C. § 103 as unpatentable over U.S. Patent No. 6,671,805 to Brown et al. (hereinafter Brown) in view of a newly cited Bull et al. literature document (hereinafter Bull). Claims 3 and 10 stand rejected under 35 U.S.C. § 103 as unpatentable over Brown and Bull, further in view of U.S. Publication 2003/0145197 to Lee et al. (hereinafter Lee). These rejections are traversed on the ground that neither of the proposed combinations would result in a document management system or method that satisfies all of the requirements of any of Applicants' pending claims.

By way of an illustrative example disclosed in the present application, an electronic document is divided into two or more partial documents (e.g. at step 115 in FIG. 4), and items 302 or 304 of information are generated for verifying validity for the respective partial documents. Examples of the items of information include hash functions 302a-302d for the respective partial documents 300a-300d (step 133 in FIG. 6) and signatures 304a-304d for the respective partial documents 300a-300d (step 134 in FIG. 6). The disclosed technique also involves generating an aggregate of the generated items of information (step 135 in FIG. 6), and

generating a digital signature 303a or 303b to the aggregate of the generated items of information (step 136 in FIG. 6). In the illustrated example of FIG. 2, the unmasked data 2 and signature-related data 4a or the unmasked data 2 and signature-related data 4b are combined and saved as the whole data 3. The partial documents may be masked, e.g. so that the electronic document is partially rendered private at the time of its disclosure. However, the validity of the masked electronic document (FIG. 3) can be verified, by verifying the aggregate (302a-302b or 304a-304b) of the generated items of information using the digital signature (303a or 303b).

As shown in application FIG. 7, the disclosed document management also provides a determination of whether or not each respective partial document has been deleted or modified. Step 143 is a check the signature-related data 4 to determine the type of signature technique employed in generating the items of information. If hashing was employed, then step 144 is performed to determine the hash values for all the units 300 of the unmasked data 2. Step 145 is performed to verify the units of masking 300 (partial documents) by comparing the hash values certified by aggregate signature verification in step 142 against the hash values determined in step 144. If the two hash values are equal for a respective partial document or 'unit' 300, then the validity is certified because the corresponding unit 300 is neither masked nor altered. If, on the other hand, the two hash values are not equal for a respective partial document or 'unit' 300, it means that the corresponding unit 300 is masked or altered. By contrast, if the signature technique was used (alternate branch out of step 143), then in step 146, the signature value certified by signature verification in step 142 is used to perform signature verification for each corresponding hash. If signature verification is successful, the validity is certified because each corresponding unit 300 is neither masked nor altered. If, on the other hand, signature verification

is unsuccessful, the corresponding unit 300 is masked or altered. The specification discusses these processing steps of Fig. 7, starting on line 11 of page 20 and ending on line 14 of page 22.

With that background, consider now the requirements of the pending claims. Independent method claim 8 recites, ***inter alia***:

> generating a plurality of items of information, each item of information being for verifying the validity of a respective one of the partial documents;
>
> generating an aggregate of the generated items of information for verifying the validity of the electronic document;
>
> generating a digital signature to the aggregate of the generated items of information;
>
> masking the electronic document by deleting or modifying one or more partial documents, after generating the items of information and the digital signature; and
>
> verifying the validity of the masked electronic document which has one or more deleted or modified partial documents by verifying the digital signature using the aggregate of the generated items of information, and examining the validity of each of the partial documents of the masked electronic document including the one or more deleted or modified partial documents by:
>
> > verifying the generated item of information for each respective one of the partial documents, and
> >
> > determining whether each respective partial document has been deleted or modified based on the verifying of the generated item of information for the respective partial document.

Hence, the method of claim 8 involves generating items of information for verifying the validity of respective partial documents; and the claim specifically recites determining whether each respective partial document has been deleted or modified based on the verifying of the generated item of information for the respective partial document. The method of claim 8 also involves generating an aggregate of the items of information, generating a digital signature to the aggregate and verifying the validity of the masked electronic document in part by verifying the digital signature using the aggregate of the generated items of information. Although the

wording (and thus claim scope) varies somewhat, the independent apparatus claim 1 recites functions of the system elements that are similar to these steps of method claim 8. It is respectfully submitted that neither the combination of Brown and Bull nor the combination of Brown, Bull and Lee would satisfy all of these claim aspects for verifying the validity of the masked electronic document.

Brown discloses an electronic document that is composed of one or more to-be-signed portions, an access-restricted portion and a processing portion (Fig. 1, Fig. 6 and col. 15, lines 17-21). Brown generates a digital signature for the to-be-signed portion to verify the validity of that portion, but Brown generates nothing for the access-restricted portion and the processing portion. That is, Brown does not teach what corresponds to the plurality of items of information for verifying the plurality of partial documents, of Applicants' independent claims. Since Brown does not generate such items of information, Brown does not teach a digital signature for the aggregate of the generated items of information. In addition, since Brown generates a secret message digest for the to-be-signed portion after masking the access-restricted portion, the masked portion is out of the target for verification.

Bull discloses a system dealing with Content Extraction Signature (CES) where a signer (Ace University), a document owner (student Bob) and a verifier (employer) are involved. The signer produces an original document divided into two or more partial documents and generates a digital signature for the whole document. The document owner receives the original document, produces an extracted document (subdocument) from it by deleting (extracting) or modifying (blinding) one or more of the partial documents and generates a digital signature (extracted signature) for the subdocument. The verifier receives the subdocument, verifies the

subdocument to see whether it complies with a predetermined extraction policy and verifies the extracted signature.

The document owner in Bull produces the extracted signature from the digital signature the signer has signed. As for each of the deleted partial documents, the document owner generates a hash value (digest value) for the partial document to be deleted. This process can be easily done for anyone because no special information, such as a secret key, is needed.

The subject matter of independent claims 1 and 8 is characterized by the signature device or step generating a plurality of items of information (such as hash values or signature values), where each item of information is for verifying validity of a respective one of the partial documents (masking units). That is, each partial document is accompanied with a hash value, signature or the like to facilitate the verification of the respective partial document. In contrast, the partial documents in Bull do not have the hash values or signature values with them.

In Bull, the <Digest> element corresponds to a hash value. However, the <Digest> element is one that the document owner generates for each partial document to be deleted when producing the extracted signature (page 6 of 15 in Bull, the last paragraph). Hence, it is evident that the original document or original portion(s) thereof does not carry <Digest> elements with it. Only the deleted partial documents have them, but the rest of the partial documents do not.

As claimed, the items of information not only exist for the original document portion(s), but also exist for the partial documents not deleted after making operation. This feature is disclosed in Applicants' FIG. 2 and FIG. 3. Regarding the verification operation, the disclosed technique has a process of set 145, as shown in FIG. 7, that examines whether the hash value 302 held as signature-related data coincides with a hash value calculated on a masking unit in step 144. On the other hand, Bull could not make this comparison because there is no hash value to

be held in Bull. Note that the first conditional branch in Bull's Fig. 4 (Verify Policy transform algorithm) examines whether a fragment element has a <Digest> element or not.

Checking the masking unit in Applicants' disclosed step 145 makes it possible to tell which of the masking units has been altered (specification p. 21, line 19 to p. 22, line 2). Thereby, the partial documents that are successful in verification or validly masked can be displayed in a way that distinguishes from other partial documents (e.g. altered units). In Bull, when the electronic document has been altered, Bull can tell there is an alteration anywhere in the whole document, but it cannot identify the position at which the document has been altered.

Hence, the combination of Brown and Bull would still not satisfy the requirements for verifying the validity of the masked electronic document by both (1) verifying the digital signature using the aggregate of the generated items of information and (2) determining whether each respective partial document has been deleted or modified based on the verifying of the generated item of information for the respective partial document. Since Brown in combination with Bull does not meet all requirements of either independent claim 1 or independent claim 8, those claims and the various dependent claims patentably distinguish over that combination.

The further addition of Lee would not overcome the above noted deficiencies in the base combination of Brown and Bull. The Office Action cited Lee only for a verification display function. Addition of such a display function to the combination of Brown and Bull still would not overcome the deficiencies of Brown and Bull or result in a system or method that verifies the validity of the masked electronic document by both verifying the digital signature using the aggregate of the generated items of information and determining whether each respective partial document has been deleted or modified based on the verifying of the generated item of information for the respective partial document, as required by independent claims 1 and 8.

Claims 1 and 8 would be patentable over Brown, Bull and Lee, therefore dependent claims 3 and 10 that were rejected over that three-reference combination should also be patentable.

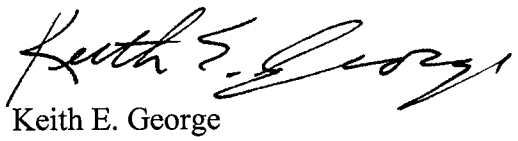
Upon entry of the above claim amendments, claims 1, 3-8 and 10-16 are active in this application, all of which should be definite and should be patentable over the art applied in the latest Action for at least the reasons presented above. The utility rejection also should be withdrawn in view of the remarks above. Applicants therefore submit that all of the claims are in condition for allowance. Accordingly, this case should now be ready to pass to issue; and Applicants respectfully request a prompt favorable reconsideration of this matter.

It is believed that this response addresses all issues raised in the September 14, 2007 Office Action. However, if any further issue should arise that may be addressed in an interview or by an Examiner's amendment, it is requested that the Examiner telephone Applicants' representative at the number shown below.

To the extent necessary, if any, a petition for an extension of time under 37 C.F.R. § 1.136 is hereby made. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account 500417 and please credit any excess fees to such deposit account.

Respectfully submitted,

McDERMOTT WILL & EMERY LLP



Keith E. George
Registration No. 34,111

Please recognize our Customer No. 20277 as our correspondence address.

600 13th Street, N.W.
Washington, DC 20005-3096
Phone: 202.756.8000 KEG:apr
Facsimile: 202.756.8087
Date: March 14, 2008